

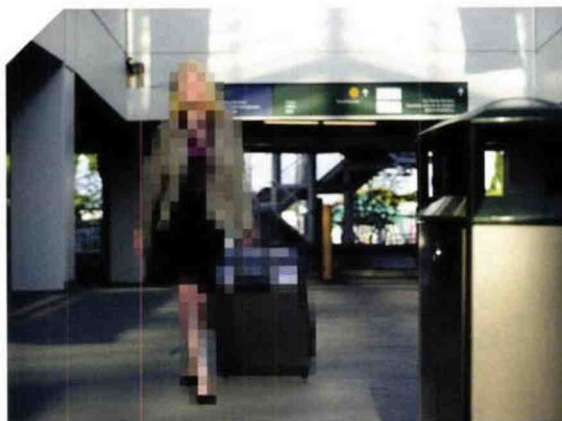


# Promouvoir la sécurité EN PROTÉGEANT LA VIE PRIVÉE ET LES LIBERTÉS

Avec la progression de l'interconnexion, les données numériques sont de plus en plus omniprésentes et personnelles. L'impact financier de la cybercriminalité est indéniable, et des groupes organisés aux moyens considérables ont remplacé les hackers solitaires au rang des cybermenaces les plus graves. Les attaques sont donc plus sophistiquées et exigent par conséquent des défenses de sécurité plus complexes. Protéger son entreprise, c'est s'assurer de pouvoir faire face à de nouvelles menaces. Genetec n'a de cesse depuis 1997, de s'adapter à ce monde de plus en plus instable et d'accompagner les acteurs dans une démarche globale.

PAR CÉLINE BRUNETAUD

Genetec a démarré dans le domaine de la vidéoprotection, en surfant sur la vague de l'innovation liée à la vidéo sur IP. « Notre conviction a toujours été celle que les technologies peuvent éliminer les obstacles et élargir les perspectives dans un monde toujours en mouvement. Notre tout premier système de vidéoprotection IP était fidèle à cette conviction. La sécurité physique et publique évolue sans cesse et nous avons notamment été précurseurs sur les sujets de la cybersécurité et du respect de la vie privée devenus de plus en plus présents au cœur des questions de vidéoprotection et de sécurité au sens large », explique Cyrille Becker, directeur général Europe de Genetec. Le secteur de la sécurité physique n'a pas échappé à la complexification des environnements informatiques, notamment avec la multiplication des systèmes et des objets connectés, et leur connexion et interconnexion. Il présente une surface d'attaque étendue pour les cybercriminels, qui peuvent plus facilement accéder aux réseaux et aux données des entreprises et institutions. « Pour y remédier, nous intégrons plusieurs couches de défense dès la conception de nos solutions, garantissant qu'elles ne deviendront pas le maillon faible permettant de compromettre les systèmes et données de l'entreprise. » ajoute Cyrille Becker.



## CHIFFREMENT, AUTHENTIFICATION, AUTORISATION

Parmi les principales couches de défense incluses dans les solutions Genetec : le chiffrement, qui permet de masquer et de protéger les données contre les utilisateurs non autorisés et de sécuriser la communication entre les clients et les serveurs ; l'authentification, qui permet de déterminer qu'une entité (serveur ou poste client) est bien celle qu'elle prétend être, et de vérifier si et comment elle peut accéder aux systèmes ; et l'autorisation, qui permet de limiter les activités au sein des systèmes, en accordant des droits d'accès spécifiques à des individus ou groupes d'individus, en fonction de leur rôle dans l'entreprise. « Nous avons donc développé une plateforme de solutions unifiées de sécurité incluant le contrôle d'accès et la lecture de plaque d'immatriculation en sus de la vidéoprotection ». Genetec pense donc la sécurité dans sa globalité au travers de Security Center, cette plateforme unifiée de sécurité qui permet aux utilisateurs de disposer d'un produit unique pour la gestion complète de leur système de sécurité. Disposant d'une même interface intuitive, la plateforme procure

S&amp;d Magazine



une meilleure vue d'ensemble et une meilleure connaissance situationnelle de la sécurité physique. Basée sur une architecture ouverte, *Security Center* permet de capitaliser sur leur équipement de sécurité existant, et de le faire évoluer au rythme des besoins du client, sans contrainte. En 2018, *Security Center SynergisMC* a reçu le plus haut niveau de la certification de sécurité de premier niveau de l'Agence nationale de la sécurité des systèmes d'information (ANSSI). « C'est une véritable reconnaissance des efforts mis en oeuvre pour garantir la cybersécurité de nos produits. Le processus de certification, avec son analyse de conformité et ses tests de pénétration, est très strict et totalement impartial. Nous avons ainsi la preuve de la robustesse de nos produits sécurisés », se réjouit Cyrille Becker. Une garantie essentielle alors que Genetec est présent dans les secteurs pétroliers et gaziers, les aéroports ou encore les institutions financières. L'entreprise dote également des villes, des opérateurs de transport, des forces de l'ordre, des préfectures, des ministères ou encore des hôpitaux.

## TENDANCES 2020 – IA : DISTINGUER LA RÉALITÉ DE LA FICTION

En matière de sécurité physique, plusieurs tendances se dégagent sur le moyen et long termes : l'intelligence artificielle, la reconnaissance faciale, la gestion des identités physiques et la blockchain. Alors que l'intelligence artificielle devient un buzz word, elle est encore loin d'être une réalité pour tous. Bien que les machines progressent à grands pas, elles ne sont pour l'heure pas capables de penser ou d'agir comme des humains. En revanche, elles sont très douées pour passer au peigne fin une grande quantité de données et fournir des informations plus approfondies afin d'aider à la prise de décisions plus éclairées, plus rapidement et plus efficacement. En 2020, le *machine learning* devrait continuer à fortement progresser dans le secteur de la sécurité, « aidant les villes et les forces de l'ordre à déployer leurs ressources physiques plus efficacement en fonction des prévisions de criminalité. » souligne Cyrille Becker. Le *machine learning* sera également déterminant pour aider les systèmes de reconnaissance automatique de plaques d'immatriculation à devenir plus performants en matière de lecture de caractères, de rejet des lectures erronées, de reconnaissance de l'origine d'une plaque d'immatriculation, etc.

46

## RECONNAISSANCE FACIALE : CONJUGUER PROTECTION ET CONFIDENTIALITÉ

Quant à la reconnaissance faciale, le sujet est plus complexe, notamment à cause du cadre législatif encore en discussion et des questionnements sur l'atteinte à la vie privée. Chez Genetec, des solutions de pointe développées par leurs partenaires sont d'ores et déjà intégrées du point de vue technologique pour améliorer la sécurité. Les déploiements, quant à eux, se font dans le strict respect de la loi.

« Nous pensons qu'en travaillant de concert avec les organismes de réglementation, il est possible de conjuguer protection et confidentialité, par le floutage des vidéos en temps réel par exemple. Ces solutions utilisent une approche de confidentialité dès la conception afin de dissiper les inquiétudes et d'accroître la protection. » estime Cyrille Becker. La gestion des identités physiques va également se démocratiser. Jusqu'alors très onéreux, ce type de solution est désormais plus accessible, notamment grâce à l'avènement du cloud. Cela va permettre d'améliorer le contrôle d'accès grâce à l'automatisation de la gestion des demandes et - surtout - des révoqueries d'accès.

## PROTECTION DES DONNÉES ET BLOCKCHAIN

Afin de prévenir les menaces, la blockchain sera, elle aussi, de plus en plus utilisée. « Elle permet de suivre l'évolution des données dans le temps, de manière non destructive. En raison de sa capacité à retracer les interactions avec des fichiers numériques, la blockchain peut déterminer si un fichier a été altéré, puis fournir des informations sur le lieu et l'heure où ce « sabotage » s'est déroulé. Dans le secteur de la sécurité physique, elle est incroyablement puissante lorsqu'il s'agit de maintenir la chaîne de responsabilité et de s'assurer que les données de sécurité n'ont pas été manipulées. »

La cybersécurité continuera d'être un enjeu massif pour l'industrie de la sécurité physique en 2020. Plus les entreprises collecteront de données, plus elles auront de données à protéger. Aujourd'hui, les instances dirigeantes et les fabricants responsables travaillent déjà en partenariat avec des chercheurs universitaires, des experts en technologie, des défenseurs des droits civils et des dirigeants de l'industrie pour réglementer l'utilisation de technologies potentiellement invasives et les procédures requises pour se prémunir contre les violations de données. Ces partenariats continueront à se renforcer en 2020.

« En plus d'aider à orienter la réglementation, les fabricants devront investir massivement dans la cybersécurité en intégrant par défaut des protections dans leurs produits. Pour toutes les parties concernées, l'objectif sera de promouvoir la sécurité tout en protégeant la vie privée et les libertés civiles des individus. Ce n'est qu'à cette condition que nous pourrions profiter des deux en même temps. » conclut Cyrille Becker.

La cybersécurité continuera d'être un enjeu massif pour l'industrie de la sécurité physique en 2020.